

REMARKS

Claims 1 to 8, 10 to 15, 18 and 19 are pending in the application. This amendment amends claims 1, 3 to 6, 10, 11, 14, 15, and 18, and cancels 9, 16, 17, and 20. The amendments to independent claims 1 and 11 have been made in an effort to expedite the prosecution to allowance or, in the alternative, to place the application in better condition for appeal. More particularly, the limitations of claims 16 and 17 have been incorporated into claim 11 and similar limitations have been added to claim 1.

The claimed invention is to a system and method for operating a car rental system, generally shown in Figure 1, which includes a reservation server 110. A user of the car rental system accesses the system over a network, such as the Internet 120, or at a kiosk 140 of the car rental system. The user is first authenticated by the reservation server, as indicated by step 202 of Figure 2. Once authenticated, the reservation server prompts the user for date, time, and location for pickup and return, and type of car requested. The user input is received at step 206, and the server checks availability of the type of car requested and, if a suitable car is available, creates a digital key for a car. More particularly, the server obtains vehicle and user information, combines this information and signs it with a digital signature using a private key of the reservation server as a digital signature of the reservation server, as shown in steps 210 to 216. The digital key is downloaded in step 220 to a portable storage device to be used by the user to gain access to the rental car. Each car of the fleet includes an in-car access controller, generally shown in Figure 3, which has a slot 342 for receiving the portable storage device. The in-car access controller detects insertion of the portable storage device in a slot and reads the digital key stored on the portable storage device and, if the digital key is not yet invalidated, verifies the digital signature of the reservation server on the digital key, and if the digital signature of the reservation server is verified by the in-car access controller, prompts the user to enter personal information identifying the user, typically a personal identification number (PIN) using PIN pad 344. This is shown in Figure 4 at steps 402 to 410. The in-car access controller checks the personal information identifying the user

(e.g., PIN) entered by the user against the personal information identifying the user of the digital key and, if the personal information identifying the user entered by the user does not match the personal information identifying the user of the digital key, the digital key is invalidated by the in-car access controller (step 418), but if the personal information identifying the user entered by the user matches the personal information identifying the user of the digital key, the in-car access controller activates instruments which the user is authorized to have access to (step 414). Upon receiving a request from the user to return the car, the in-car access controller obtains car status information, including fuel level, mileage, current time and car ID, and creates a return packet by combining car status information and current digital key and signing the return packet using a private key of the in-car access controller as a digital signature. This is shown in steps 504 to 510 of Figure 5. The in-car access controller saves the return packet on the portable storage device (step 512) and invalidates the current digital key (step 514). The rental transaction is completed at the car rental center at a kiosk which retrieves the return packet from the portable storage device, as shown at step 604 in Figure 6, and prints a receipt for the user in step 614.

Claim 11 was rejected under 35 U.S.C. §112, second paragraph, as being indefinite. The Examiner states that the recitation of “checking by the reservation server an availability of a requested car and, if a car is available, creating by the reservation server a digital key by car and user information with a digital signature of the reservation server” is unclear to him. Claim 11, in addition to being amended to include the limitations of claims 16 and 17, has been amended to make clear the intended limitation. As amended, it is submitted that claim 11 is no longer subject to this ground of rejection, and withdrawal of the rejection is respectfully requested.

Claims 1 to 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0013815 of Obradovich et al. in view of U.S. Patent No. 6,380,842 to Mattes et al. This rejection is respectfully traversed as to the claims in their presently amended form.

In making this rejection, the Examiner asserts that “Obradovich discloses the system wherein a renter of a car invalidates a valid digital key upon returning

a car to the car rental system and presents an invalidated digital key to the key return system to complete a car return”, citing page 10, paragraph 0106, of Obradovich et al.; however, the Examiner is in error. The cited paragraph deals only with the access code for the E-card used by the driver. There is nothing in this paragraph, nor for that matter in any other part of the reference, of invalidating a digital key. Invalidating the digital key is part of the process of generating the return process which includes storing a return packet on the portable storage device. See Figure 5. This return packet is accessed to generate and print a receipt for the user. See Figure 6.

Claim 11, as amended, recites “upon receiving a request from the user to return the car, obtaining by the in-car access controller car status information, including fuel level, mileage, current time and car ID, and creating by the in-car access controller a return packet by combining car status information and current digital key and signing the return packet using a private key of the in-car access controller as a digital signature, and saving by the in-car access controller the return packet on the portable storage device; and invalidating the current digital key and printing a receipt for the user.” Nothing like this is contemplated by Obradovich et al. Claim 1 similarly recites that “the in-car access controller . . . [is] responsive to a request from the user to return the car and . . . [includes] means for obtaining car status, including fuel level, mileage, current time and car ID, and . . . [generates] a return packet by combining car status information and current digital key and . . . [signs] the return packet using a private key of the in-car access controller as a digital signature and . . . [saves] the return packet on the portable storage device”.

The Examiner relies on Mattes et al. for a suggestion of a “system having each of said fleet of cars being capable of invalidating a digital key”, citing column 5, lines 25-64. On the contrary, Mattes et al. suggests nothing of the sort. What Mattes et al. disclose is an electronic key having a transmitter/receiver for transmitting at least one coded operating signal generated by the electronic key to a vehicle locking system. Actuating members are provided on the key and operated by the user to cause the transmitter/receiver to transmit the coded operating signal. The passage cited by the Examiner relates to additional security

wherein the key can be programmed with an additional individual code by the user which, in the active state, blocks transmission of the coded operating signal, but in the inactive state, allows transmission of the coded operating signal. There is, in fact, no invalidating of a digital key as specifically disclosed and recited in the claims of this application.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1 to 8, 10 to 15, 18 and 19 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'C. Lamont Whitham', is written over a horizontal line.

C. Lamont Whitham
Reg. No. 22,424

Whitham, Curtis, Christofferson & Cook, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743